

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MONTANA  
GREAT FALLS DIVISION**

IN THE MATTER OF THE SEARCH  
OF INFORMATION ASSOCIATED  
WITH **jandjfabrications@gmail.com,**  
**pstanford511@gmail.com,**  
**mikeolson755@gmail.com** THAT IS  
STORED AT PREMISES  
CONTROLLED BY GOOGLE, INC.

MJ-17-35-GF-JTJ

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Jared S. Thompson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, Inc. (Google), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since March, 2008. Currently, I am assigned to the Shelby, Montana RA, and part of the Salt Lake City Field Office. My experience as an FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud and intrusion. I have received training and gained experience in interviewing and interrogation techniques, arrest

procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures.

2. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), 2511(1)(a), and 2511(1)(d) have been committed by or have been caused to be committed by Julius Edward Lupowitz using the e-mail accounts jandjfabrications@gmail.com, pstanford511@gmail.com, mikeolson755@gmail.com. There is also probable cause to search the above accounts, further described in Attachment A, for the items specified in Attachment B, which constitute evidence, instrumentalities, or fruits of the foregoing violations.

### **JURISDICTION**

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703 (c)(1)(A). Specifically, the United States District Court for the District of Montana is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **BACKGROUND CONCERNING E-MAIL**

5. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“e-mail”) access, to the public. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the e-mail accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes

under investigation because the information can be used to identify the account's user or users.

6. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

7. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers, and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

8. In my training and experience, although the personal identifying information requested by an e-mail provider from a subscriber is not validated and can be easily falsified, the contents of e-mail communications can contain the subscribers true information, such as name, address, telephone number, and other email addresses and communications facilities used by a subscriber. Further, the contents of email messages can contain identifying information of other unknown subjects and additional victims. The contents of emails can also hold written conversations between the subscriber and his/her contacts discussing activities related to the crimes under investigation. Therefore, in my training and experience, the information found in the contents of email messages may constitute evidence of the crimes under investigation because such information can be used to identify subjects, accomplices, additional victims, and further details about the crimes under investigation, such as motives and methods.

9. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP

addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

10. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

### **SUBPOENA INFORMATION**

11. On February 8, 2017, a grand jury subpoena was sent to Google, Inc. for multiple email addresses to include jandjfabrications@gmail.com, pstanford511@gmail.com, mikeolson755@gmail.com, and jedlup@gmail.com. On February 11, 2017, Google, Inc. responded to the subpoena and provided subscriber information for multiple email accounts to include jandjfabrications@gmail.com, pstanford511@gmail.com, mikeolson755@gmail.com, and jedlup@gmail.com.

12. Email address jandjfabrications@gmail.com was created on September 6, 2011. The subscriber provided a recovery email account jedlup@gmail.com. 108.189.243.85 was the IP address recently used to access the account.

13. Email address pstanford511@gmail.com was created on November 20, 2010. The subscriber provided a recovery email account noah.zebi@gmail.com.

14. Email address noah.zebi@gmail.com was created on August 11, 2010. The subscriber provided a recovery email account info04@spray-lining.com. The subscriber provided SMS telephone number 321-704-4496.

15. Email address mikeolson755@gmail.com was created on August 18, 2010. The subscriber provided a recovery email account jedlup@gmail.com. The subscriber provided SMS telephone number 321-848-3013.

16. Email address jedlup@gmail.com was created on December 19, 2010. The subscriber provided a recovery email account je4@spray-lining.com. The

subscriber provided SMS telephone number 321-704-4496 as associated with the jedlup@gmail.com account. 108.189.243.85 was the IP address recently used to access the account.

17. Vonage Holdings Corporation (“Vonage”) provided telephone records in response to a separate grand jury subpoena. Telephone number 321-704-4496 is one of several telephone numbers associated with Vonage account number 34417 (“the Vonage Account”), Account Name Safe Tech Group, Jed Upowi, address 4155 Dow Rd, Unit J, Melbourne, Florida 32934, email address je4@spray-lining.com. Billing information for the Vonage account identifies a VISA Credit Card, with 9852 as the last four digits, in the name of Julius Lupowitz, with the same address listed above.

18. Subsentio, on behalf of Bright House Networks, identified IP address 108.189.243.85 as assigned to customer Green Tech Solutions Team Inc., address 4155 Dow Rd, Ste J, Melbourne, FL 32934 as of February 7, 2017. As of March 17, 2017, the account was identified as currently active. There were several partially identified credit cards listed in the method of payment section. “WSC Visa Card X9852, Exp 1/31/20” was one of the cards listed.

19. Several financial institutions (e.g. Bank of America, JP Morgan Chase, SunTrust Bank), have provided records in response to grand jury subpoenas. “Safe Tech Group Inc” was the account title or corporate name listed with the Bank of America records. Green Tech Solutions Team Inc. was the account title for the JPMC and SunTrust Bank records. Julius Lupowitz is the only person listed as a signer for the accounts. Lupowitz is listed as the President/secretary in the Bank of America records, and listed as President in the JP Morgan Chase and SunTrust bank records.

## **FACTS ESTABLISHING PROBABLE CAUSE**

### **A. Incident Description**

Julius Edward Lupowitz (Lupowitz) using other aliases, both known and unknown, is affiliated with a company named Spray-Lining, a Division of Flexible Lining Systems. In short, Lupowitz uses his company to hire new “dealers,” who subsequently receive large customer orders and often then order a specific needed product through Lupowitz. The customer eventually disappears and the victim dealer is left with product purchased from Lupowitz.

### **The Set-Up:**

Lupowitz contacts individuals (hereinafter referred to as “victim dealers”) who have made an inquiry into the Spray-Lining.com (Flexible Lining Systems) company. The company maintains a website. The company represents to manufacture a polyurea, epoxy-type product similar to Rhino Linings and Line-X Bedliners. Lupowitz’s sales pitch to the victim dealer is that the local dealer in the area who distributes Spray-Lining product is no longer serving as the local dealer because of different reasons (e.g. prior dealer violated his contract agreement, is no longer working because of health reasons, or relocated) and the area has an opening.

Lupowitz, typically through an alias, makes a high pressure sales pitch to the the victim dealer to buy the rights to be the exclusive dealership for his products in the area where the victim dealer lives. The cost to be the exclusive dealer has ranged from \$3,500 to \$10,200.

Victim dealers are often then directed to or request to talk with the prior dealer as a reference. One victim dealer, Mark Stephens, from Dutton, Montana requested to visit with the prior dealer identified as “Leroy Tubbs” and was provided his contact number by Lupowitz (who used the alias J. Randy Lance). This telephone number 623-399-4568 for “Tubbs” is one of the numbers included in the Vonage Account. This number is also the same phone number given to another victim dealer, Michael Hemingway, to contact a former sales representative named “Kurt.” Further, victim dealer Geoff Feltham contacted a prior dealer named “Leroy” using the same telephone number who was reportedly located in Flagstaff, Arizona.

Stephens spoke to “Tubbs” and “Tubbs” confirmed the story Lupowitz gave Stephens - “Tubbs” was a former dealer for Line-X products and Spray-Lining products, but was now no longer employed by Spray-Lining. “Tubbs” was the supposed Line-X dealer for the Great Falls, Montana area. However, in contacting the regional sales representative for Line-X, Samantha Styger, advised there is no “Leroy Tubbs” at all in their records for the last ten years to include any “Leroy Tubbs” working as a Line-X distributor in the Great Falls, Montana area. Further, Line-X had neither a location nor a distributor in the Great Falls area.

Another victim dealer, Robin Milender, from Evanston, Wyoming, contacted the prior dealer in his area, named “Leroy last name unknown (LNU)”, who apparently worked for both Rhino Lining products and Spray-Lining. “Leroy LNU” spoke to Milender and said he was working out of the Salt Lake City area. Lupowitz, again using the alias of J. Randy Lance, explained “Leroy LNU”



obtained jobs from Flexible Lining (or Spray-Lining) and used the Rhino Lining product for those jobs. As a consequence, “Leroy LNU” lost his Spray-Lining dealer status for that area. When victim dealer Milender contacted “Leroy LNU,” “Leroy LNU” confirmed the story Lupowitz provided. Leroy LNU had since relocated to Arizona.

Another victim dealer, Michael Hemingway, from Vermont attempted contact with the prior dealer in his area of Plattsburg, New York, “Kurt last name unknown (LNU).” Kurt LNU was moving to Arizona due to health issues. Lupowitz, again using the name Randy Lance, provided Hemingway a telephone number to contact Kurt LNU. Hemingway attempted to call Kurt LNU but was unsuccessful. The telephone number Lupowitz provided Hemingway to contact Kurt LNU was 623-399-4568 - the same number victim Stephens used to contact Leroy Tubbs. The Vonage Account records identify Milender’s cellular telephone number 307-679-1361 called the same number 623-399-4568 on March 13, 2014.

***The Customer and Buy from Lupowitz:***

Sometime after buying an exclusive dealer status, a “customer” contacts the victim dealer regarding a job opportunity usually by email but some victim dealers also had telephonic conversations with the customer. The job is typically a big industrial job from a vendor not in the local area to coat a large number of pieces or parts. Multiple victim dealers (e.g. Stephens and Milender) had customer contact from a person named “Pete Stanford” using the email address pstanford511@gmail.com. The victim dealers were provided telephone number 647-367-9506 to call Pete Stanford with “Agent Contracting.” His phone number, 647-367-9506, is included in the same Vonage Account. His email address, name and telephone number are the same for the customer who contacted Mark Stephens in Dutton.

The customer tells the victim dealer about the large industrial job (several parts that need coating) that needs to be done quickly. The items need to be coated with a specific product which Spray-Lining provides. Lupowitz then assists the victim dealer in preparing a bid for the project and the victim dealer submits the bid to the customer. The customer conveys to the victim dealer that they have the job if they will complete it by the narrow timeframe. The customer required multiple victim dealers to provide them a certificate verifying they have purchased the product.

Under the pressure to be ready, the victim dealer orders the needed product from Spray-Lining. Lupowitz explains to the victim dealer that the product has to be paid for upfront. Some victims (e.g. Milender) expressed to Lupowitz about not having the funds to buy the entire product needed to complete the job. Lupowitz explains his company, Spray-Lining, will finance part of the cost, and the victim dealer (e.g. Milender) only needs to come up with a portion of the cost. The product is ordered by the victim dealer and Lupowitz is paid.

In some cases, the customer then informs the victim dealer that the job size just became much bigger. If the victim dealer wants to keep the job, they will need to coat a larger batch of pieces. In the rush to keep the job and turn around the project quickly, the victim dealer subsequently contacts Lupowitz and explains the situation. Lupowitz advises that Spray-Lining can provide the necessary coating material for the additional items to be coated. Again, the product purchased needs to be paid for upfront, (or in Milender's case, a portion of the cost needs to be paid for upfront). The victim dealer subsequently orders and purchases more material from Lupowitz to satisfy the customer's order.

Often, the customer also contacts the victim dealer again and informs them that the company they previously hired out to apply the primer coat on the parts is now no longer able to perform. If the victim dealer wants to keep the job, they will now need to also prime all of the parts with a primer coating material which Spray-Lining provides. The victim dealer again contacts Lupowitz and walks through the new set of facts with him. Lupowitz confirms Spray-Lining can also provide the needed primer product. The primer product will need to be paid for upfront (and in Milender's case, this time Spray-Lining will only finance 50% of the cost of the primer material – Milender is required to pay 50% of the cost upfront instead of 33%).

These products are then sent to the victim dealer, who anticipates using the product for the customer.

### **The Finish:**

The customer never delivers the items to be coated to the victim-dealer. The customer eventually stops corresponding with the victim dealer. The victim dealer is out the funds they paid to Lupowitz for the spray lining product, even though they have the product itself.



In sum, the investigation to date has identified over 20 victims with funds paid to Lupowitz exceeding \$900,000.

**B. Connection of Lupowitz to other aliases through Phone and Email Records**

Julius Edward Lupowitz explained to the investigating Agent in 2016, he used the name “Randy Lance” as his name in communicating with customers. In a deposition in March of 2008, Lupowitz advised he used the name “Eddie Lupe” in communicating with customers. As part of a response to a civil complaint in 2015, Lupowitz advised Jeff Powell was a name by which he was sometimes known in connection with his work for Green Tech Solutions Team, Inc, d/b/a Flexible Lining Systems.

In approximately 2010, Lupowitz was confronted by victim dealer Darren Wardell, located in Alberta, Canada, regarding his true identity and his scam. The name Lupowitz had been using in communicating with Wardell was Jed Upowi. Lupowitz provided Wardell a brief explanation as to why he used a different name.

Telephone numbers 972-996-7326, 321-848-3013, and 321-704-4496 are some of the numbers Lupowitz has used in communicating with victim dealers with the different names previously mentioned. 972-996-7326 and 321-704-4496 are telephone numbers included in the Vonage Account. 321-848-3013 pertains to a Verizon Wireless account for Lupowitz.

Lupowitz used email account rl@spray-lining.com when communicating by email with victim dealers and potential customers using the name Randy Lance or J. Randy Lance. Victim dealers (e.g. Mark Stephens, Robin Milender, and Benjamin Knandel) received correspondence from this email **from approximately March 2014 to March 2015.**

Je4@spray-lining.com was also one of the email addresses Lupowitz used in communicating with victim dealers. Spray Lining representative “Randy Lontz” or “J. Randy Lontz” also used email accounts rl@spray-lining.com and je4@spray-lining.com and telephone numbers 972-996-7326, 321-848-3013 when communicating with victim dealers and potential customers (e.g. Kristofer Johns, Michael Ray, Brad Galbraith, M G Bryan Equipment and William Metcalf) from approximately from approximately August 2015 to January 2017. Using the name

Eddie Lupe, Lupowitz communicated with victim dealer Scott Oppor using email address jedlup@gmail.com.

“Prior dealers” or references for Spray-Lining provided by Lupowitz and the individual who identified himself as “Randy Lontz” to victim dealers and others include the following names with associated telephone numbers.

“Leroy Tubbs”	623-399-4568
“Kurt”	623-399-4568
“Leroy Tubbs”	480-389-0144
“Curt McClintock”	312-361-8467
“Billy Foster”	206-607-6715
“Blake Edison”	647-367-9506
“Willy Sivers”	281-408-4266
“Lee McClintock, aka Leroy”	480-389-0144
“Ryan at National”	267-546-5372
“Leroy”	623-399-4568

“Customers” who have contacted victim dealers with large industrial jobs include the following names with associated telephone numbers and email accounts:

“Pete Stanford”	647-367-9506	<b>pstanford511@gmail.com</b>
“Paul Stanford”	647-367-9506	<b>pstanford511@gmail.com</b>
“Pete Stanford” and		
“Nick Bolescue”	647-367-9506	<b>pstanford511@gmail.com</b>
“Mike Olson”	808-664-3817	<b>mikeolson755@gmail.com</b>
“Jason Fistron”	587-883-9633	jfistron@gmail.com
“Michael J. Bradley”	587-883-9633	<b>jandjfabrifications@gmail.com</b>
“Thomas Ladonik” and		

“Samuel Jolota”	647-367-9506	<i>jandjfabrifications@gmail.com</i>
“Kyle Rasmussen”	647-367-9506	<i>jandjfabrifications@gmail.com</i>
“Toran Levesque”	647-367-9506	<b>pstanford511@gmail.com</b>
“Mike Olson”	647-367-9506	<b>mikeolson755@gmail.com</b>
“Gary Erin” and		
“Lucian Doru”	647-367-9506	<i>jandjfabrifications@gmail.com</i>

All of the telephone numbers aforementioned for the Spray Lining prior dealers or references as well as all of the telephone numbers listed for the customers pertain to the Vonage Account.

“Pete Stanford” was a customer name provided to victim-dealers Mark Stephens and Robin Milender. “Paul Stanford” was a customer name provided to victim dealer Scott Oppor. “Mike Olson” was a customer name provided to Michael Hemingway.

Google email address information was subpoenaed for “Customer” email accounts listed above. In response Google provided the following information:

The recovery email address initially listed for *mikeolson755@gmail.com* was sandykic2@gmail.com. An Internet Protocol (“IP”) address 97.68.221.70 was used in 2015 to access the *mikeolson755@gmail.com* account. The recovery email address listed for *mikeolson755@gmail.com* from the 2nd Google request is jedlup@gmail.com. Additionally, +13218483013 was included as an SMS number for that email account. 321-848-3013 is a telephone number associated with a Verizon account for Lupowitz.

The recovery email address listed for *pstanford511@gmail.com* was noah.zebi@gmail.com. The recovery email address listed for noah.zebi@gmail.com is INF04@Spray-lining.com. Additionally, +13217044496 was included as an SMS number for that email account. 321-704-4496 is a telephone number associated with the Vonage Account.

The recovery email address listed for *jandjfabrifications@gmail.com* was jedlup@gmail.com. IP address

108.189.243.85 was recently used in February 2017 to access the account. 108.189.243.85 was the most recent (11/10/2016) IP address identified with the noah.zebi@gmail account.

Subsention provided subscriber info in behalf of Bright House Networks. IP Address 108.189.243.85 is currently assigned to customer Green Tech Solutions Team Inc, address 4155 Dow Rd, Ste J, Melbourne, Florida 32934, email address je4@spray-lining.com. The account was active as of March 17, 2017.

GoDaddy.com provided records pertaining to spray-lining.com. Contact information for spray-lining.com was the following: Login name: jlupowitz; First Name: Jules; Last Name: Lupowitz; Address 1: 4155 Dow Road; Address 2: Unit J; City: Melbourne; State/Prov: FL.

### **Relevant Electronic and Wire Communication Statutes**

17. The relevant federal statutes involved in the disclosure of customer communication records are as follows:

a. 18 U.S.C. § 2703(a) provides, in part: “A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant.”

b. 18 U.S.C. § 2703(b)(1)(A) provides, in part: “A governmental entity may require a provider of remote computing service to disclose the contents of a wire or electronic communication ... (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant.”

c. 18 U.S.C. § 2703(c)(1)(A) provides, in part: “A governmental entity may require a provider of electronic communication service or remote computing to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the

governmental entity (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent Stare warrant.”

d. 18 U.S.C § 2510(1) defines a “wire communication” as “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications affecting interstate or foreign commerce.”

e. 18 U.S.C. § 2510(12) defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce,” with certain exceptions not applicable here.

f. 18 U.S.C § 2510(17) defines “electronic storage” as “any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof;” and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication.”

## **Technical Background**

18. E-mail is an electronic form of communication which usually contains written correspondence and graphic images. It is similar to conventional paper mail in that it is addressed from one individual to another and is usually considered private. An e-mail usually contains a message “header” which generally displays the sender’s e-mail address, the recipient’s e-mail address, and the date and time of the e-mail transmission.

19. If a sender chooses to do so, he or she can type a subject line into the header. E-mail message “headers” usually contain information, such as identification of the sender’s ISP, which enables law enforcement officers to trace the message back to the original sender. In order to do so, information must be obtained from the sender’s ISP through a Grand Jury or administrative subpoena.

20. In my training and experience, I have learned that Google.com provides a variety of on-line services, including e-mail access, to the general public. Subscribers obtain an account by registering with Google.com. During the registration process, Google.com asks subscribers to provide basic personal information. Therefore, the servers of Google.com are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Google.com's subscribers) and information concerning subscribers and their use of Google.com services, such as account access information, e-mail transaction information, and account application information.

21. In general, an e-mail that is sent to Google.com subscribers is stored in the subscriber's "mail box" on Google.com's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google.com's servers indefinitely.

22. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google.com's servers, and then transmitted to its end destination. Google.com often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from Google.com's servers, the e-mail can remain on the system indefinitely.

23. Google.com's subscribers can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Google.com.

24. Subscribers to Google.com might not store on their home computers copies of the e-mails stored in their account. This is particularly true when they access their account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

25. In general, e-mail providers like these companies ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).



26. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google.com's websites), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address (IP address) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

27. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of *any* actions taken by the provider or user as a result of the communications.

### **Procedure for Search and Seizure**

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google.com to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B.

Upon receipt of the information described in Attachment B, the case agents (or other government-authorized personnel) will review all of the information. During the case agents' review of the information, the agents will segregate the information into two groups: (i) information that is the target of the warrant listed in Attachment B and which the government may therefore seize; and (ii) information that is not the target of the warrant.

Government personnel will "seize" information that is the target of the warrant listed in Attachment B by copying it onto a separate storage

device or medium. Such information may be used by law enforcement in the same manner as *any* other seized evidence.

Information that is not the target of the warrant will be sealed in a secure location. Such information will not be reviewed again without further order of the court (e.g., subsequent search warrant, or order to unseal by the district court).

29. Julius Lupowitz aka Randy Lance, amongst other known aliases, is known to have legal representation. I therefore anticipate that documents, materials, and/or electronic files potentially protected by the attorney-client privilege may be among the items found during the search. To prevent the disclosure of privileged information to case agents, investigators, and prosecutors assigned to the investigation, one agent (the “taint agent”) and one Assistant United States Attorney (AUSA) (the “taint counsel”) have been assigned to serve as a taint team to review potentially privileged material found during the execution of the warrant. The members of the taint team have had no prior involvement in the investigation, and will have no further role in the investigation or prosecution of this case, unless some further privilege issue arises requiring additional review or unless some aspect of the taint team review is litigated in court. The taint team members will not reveal the contents of any document or file determined to contain privileged material to any other person, except counsel for a subject of a search warrant or holder of a privilege, unless otherwise ordered by the court.

30. If an investigative agent finds a tangible item that may contain privileged information, that agent will not examine it further, and will immediately place it in a container identified as containing privileged information. The agent will then provide the container to the evidence custodian who will take custody of the material and seal the container for later review by the taint agent.

31. The taint agent will conduct an initial review of all documents or other tangible items identified as potentially privileged information, and determine whether such information is relevant (within the scope of the items to be seized under the warrant). If the taint team agent identifies any documents or other tangible items containing privileged information that is not relevant, the taint team agent will return such documents or other tangible items to the attorney for the holder of the privilege. If the taint team agent identifies any documents or other

tangible items containing privileged information that is relevant, the taint team agent will provide a copy of such information to the attorney for the holder of the privilege. The taint team agent will then seal the information pending conclusion of the investigation/prosecution or court order, and arrange for such information to be redacted from any information provided to investigative agents. If the taint team agent has any question about whether such information is privileged, the taint team agent will provide such information to the taint team counsel for a determination. If the taint team counsel agrees that such items contain privileged information, the taint team counsel will direct the taint team agent to provide a copy of such information to the attorney for the holder of the privilege, and to arrange for such information to be redacted from any information provided to investigative agents. If the taint team counsel has any question about whether such information is privileged, the taint team counsel will submit such information to the Court *in camera* for a judicial determination as to whether the information is privileged. If the Court deems the information to be privileged, the taint team agent will provide a copy of such information to the attorney for the holder of the privilege, and to arrange for such information to be redacted from any information provided to investigative agents.

32. Regarding any digital device or data seized, after a forensic image of such device or data is created, the taint agent will conduct an initial review of information received pursuant to the warrant to identify any potentially privileged information, and determine whether such information is relevant (within the scope of the items to be seized under the warrant). If the taint team agent identifies any privileged information that is not relevant, the taint team agent will provide a copy of such information to the attorney for the holder of the privilege. The taint team agent will then arrange for such information to be redacted from any information provided to investigative agents. If the taint team agent identifies any privileged information that is relevant, the taint team agent will provide a copy of such information to the attorney for the holder of the privilege. The taint team agent will then arrange for such information to be redacted from any information provided to investigative agents. If the taint team agent has any question about whether such information is privileged, the taint team agent will provide such information to the taint team counsel for a determination. If the taint team counsel agrees that such items contain privileged information, the taint team counsel will direct the taint team agent to provide a copy of such information to the attorney for


the holder of the privilege, and to arrange for such information to be redacted from any information provided to investigative agents. If the taint team counsel has any question about whether such information is privileged, the taint team counsel will submit such information to the Court *in camera* for a judicial determination as to whether the information is privileged. If the Court deems the information to be privileged, the taint team agent will provide a copy of such information to the attorney for the holder of the privilege, and to arrange for such information to be redacted from any information provided to investigative agents.

33. The members of the taint team will have no further role in the investigation or prosecution of this case, unless some further privilege issue arises requiring additional review or unless some aspect of the taint team review is litigated in court. The taint team members will not reveal the contents of any document or file determined to contain privileged material to any other person, except counsel for a subject of a search warrant, unless otherwise ordered by the court. The taint team agent will maintain a log of all potentially privileged material reviewed, identifying the material by type, date, sender and recipient (if applicable), and subject matter. The log will indicate whether the material reviewed is relevant, and its disposition (i.e., whether it was forwarded to the taint team counsel, sealed, or returned to the holder of the privilege).

### CONCLUSION

34. Based on my training and experience, and the facts as set forth in this affidavit, I have probable cause to believe that on Google.com's computer servers there exists evidence of violations of the above-described criminal statutes. Accordingly, a search warrant is requested

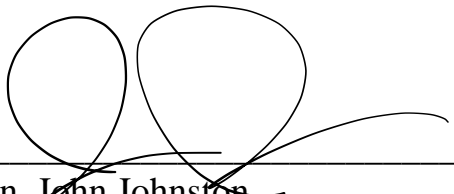
Respectfully submitted,

A handwritten signature in black ink, appearing to read "Jared S. Thompson". The signature is fluid and cursive, with the first name "Jared" being the most prominent part.

Jared S. Thompson  
Special Agent  
Federal Bureau of Investigation

Shelby, Montana

Subscribed and sworn before me this 30<sup>th</sup> of May, 2017.



---

Hon. John Johnston  
United States Magistrate Judge